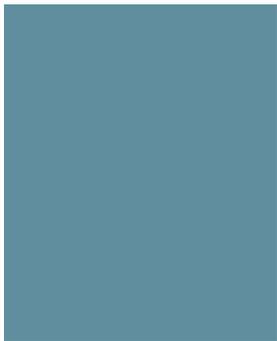




MERgE News



MERgE: Multi-Concerns Interactions System Engineering



From the Project Coordinator's Pen

With the Final Review approaching in a few months all the demonstrators are in their final stages and being evaluated. In this issue, we mention a three-day plenary with no nights and from our four domains, we have a spotlight on the Aerospace demonstrator which has several concerns specific to reliability engineering. Additionally we describe some events for security training and guidance on process engineering. We finish with a short description of one of our partner tools that can handle a great degree of architectural variants.



Thanks for your interest.

Charles Robinson

Picnic at Ainola Park Oulu

The 8th plenary meeting took place at Oulu 16th-18th of June 2016. The purpose of the meeting was to provide an opportunity for the consortium to advance in the deliverables and foster co-operation between participants. Global views on standardisation, dissemination and exploitation strategies were discussed in detail.

At these meetings we invite an external guest speaker to introduce a novel perspective. This time the participants had an opportunity to see how the tool Sirius was being utilised for developing a domain specific language by a University of Oulu PhD student. Several participants subsequently took part in a focus group to provide expert feedback for the student.

Among points discussed, especially for safety/security it can be difficult to bring processes and models into the public domain. This slows down their formalism and can block the use of current state of the art tools. Also costs can be a hindrance even given acceptability of technology by experts. Another challenge is the exchange of information between the phases of the product lifecycle. For instance dependability flaws discovered in completed systems feed back to the design stage usually only after standardisation which can take many years.



MERgE consortium members had an opportunity to witness midnight sun while having a relaxed picnic at Ainola Park at the end of a day's meeting.

INSIDE THIS ISSUE:

| | |
|---|---|
| Picnic at Ainola Park Oulu | 1 |
| Aerospace Demonstrator | 2 |
| Crash test party | 2 |
| Conforming to Software Processes and Methods | 3 |
| Cybersecurity Education—Student Challenge | 3 |
| E2S ATO tool supports trade off of thousands of design variants | 4 |

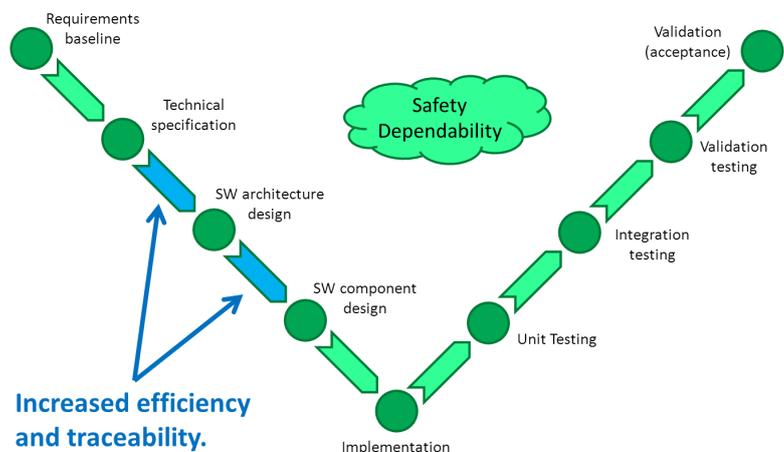
Aerospace Demonstrator

The development of on-board software for space systems is subject to strict requirements both at the technical and the process level in order to achieve the high levels of dependability and safety expected in the space domain. These requirements are driven by standards such as ECSS for European spacecraft or DO-178B for aerospace systems. Following these standards, Space Applications Services uses a toolchain based on commercial and open-source tools that cover end-to-end the phases of software development. However generally the integration of such tools is imperfect. This means manual links are required between the artefacts produced by the engineering process which is both costly and error prone.

To investigate and reduce this problem, Space Applications Services has set up, in the frame of the MERgE project, an integrated toolchain that provides multiple views of the system (architecture, dependability and safety) and maintains traceability from the requirements baseline to the software code units and tests. As shown in the image we have a particular focus between the specification to component design phases. This toolchain combines commercial software with tools specifically developed by the project partners, and supports a development process compliant with international standards.

Space Applications Services is presently evaluating the development process and the toolchain in the context of an On-Board Control Procedure (OBCP) system that is being developed for the European Space Agency. In addition, Space Applications Services relies on technologies selected for the MERgE platform to build the development environment of the OBCP system. This has proven invaluable to gain experience in model-driven software engineering.

Contributions to this use case have come from the University of Leuven, All4Tec, Pierre and Marie Curie University, University of Jyväskylä, Obeo, and the University of Oulu. One most recent advancements has been the development of a domain specific language tool providing a means to tailor the Eclipse-based modeling tools used by Space Applications Services.



Crash Test Party

The legendary Crash Test Party was held this spring at TUT (Tampere University of Technology). This time the theme was more emphasized on ICS/SCADA devices and as usual, the participant vendors were encouraged to bring their own devices to the party. The security testing tools and additional test targets were provided by Codenomicon along with a brief introduction to security testing domain followed by a full-day, hands-on 'hackathon' session. In addition to protocol fuzzers, the tool arsenal included our ISASecure solution with industry specific load testing capabilities.

Codenomicon AppCheck (static binary analysis solution) was also used to discover known vulnerabilities in ICS device firmwares. The participants included some of the major vendors and players in the field. The session proved to be very fruitful achieving lots of discussion and interest from the participants. We owe huge thanks to TUT for providing excellent facilities for this event!

By Juha Korju - Codenomicon



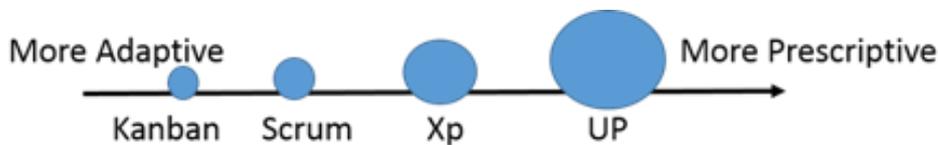
Conforming to Software Processes and Methods

UPMC (France) presented a research paper at the 30th ACM/SIGAPP Symposium On Applied Computing (SAC). This industry-driven research is conducted in the context of the MERgE project (ITEA2) and focuses on the verification of processes at design time contributing to the safety and security concerns.



The increasing complexity of engineering projects requires methodological frameworks to support development processes. A method comes with a set of best practices that are enforced and instantiated into processes to drive the realization steps of the development project. However, those best practices come in the form of text in guides and books, or they are in the developer's mind. Thus, during an instantiation of a method, there is no guaranty to enforce its best practices into the process, which could impact negatively the cost, time, and quality criteria.

Therefore, in the LIP6 team, we proposed to automatically check correct instantiation of four popular methods: Unified Process, Extreme Programming, Scrum and Kanban. The paper expands on an analysis by H. Kniberg, M. Skarin (2010) rating these methods from adaptive to prescriptive. LIP6 also proposed to check additional constraints on processes that are modeled with UML Activity Diagrams (AD). The verification is performed with model checking techniques based on fUMLsemantics.



Cybersecurity Education—Student Challenge

Team Finland from the University of Jyväskylä, Finland earned 3rd place at Europe's first Cyber 9/12 Student Challenge. In this competition which was held during April 2015 in Geneva, Switzerland sixteen teams from Finland, France, Switzerland, Poland, Hungary, Estonia, the United Kingdom, and the United States competed in order to provide their best national security policy prescriptions for combating escalating cyber conflict. This Student Challenge offered a unique venue for advancing cybersecurity education both in Europe and internationally by bringing together current and future cyber policymakers from across the transatlantic community. The competition also gathered an impressive panel of judges and many distinguished cyber experts.

The Cyber 9/12 Student Challenge is designed to offer students, across a wide range of academic disciplines, a better understanding of the policy challenges associated with cyber conflict. Part interactive learning experience and part competitive scenario exercise, the Cyber 9/12 Student Challenge gives students interested in cyber conflict policy an opportunity to interact with expert mentors, judges, and cyber professionals while developing valuable skills in policy analysis and presentation. Student teams will be challenged to respond to an evolving scenario involving a major cyber-attack and analyze the threat it poses to state, military, and private sector interests.

It must be noted that since the city of Jyväskylä was assigned a national coordinator role in cyber security the University of Jyväskylä plays a key role in the establishment of the National Cyber Security Centre of Excellence of Finland.

For further information about the Cyber 9/12 Student Challenge please visit <http://www.atlanticcouncil.org/resources/cyber-912-student-challenge-resources>



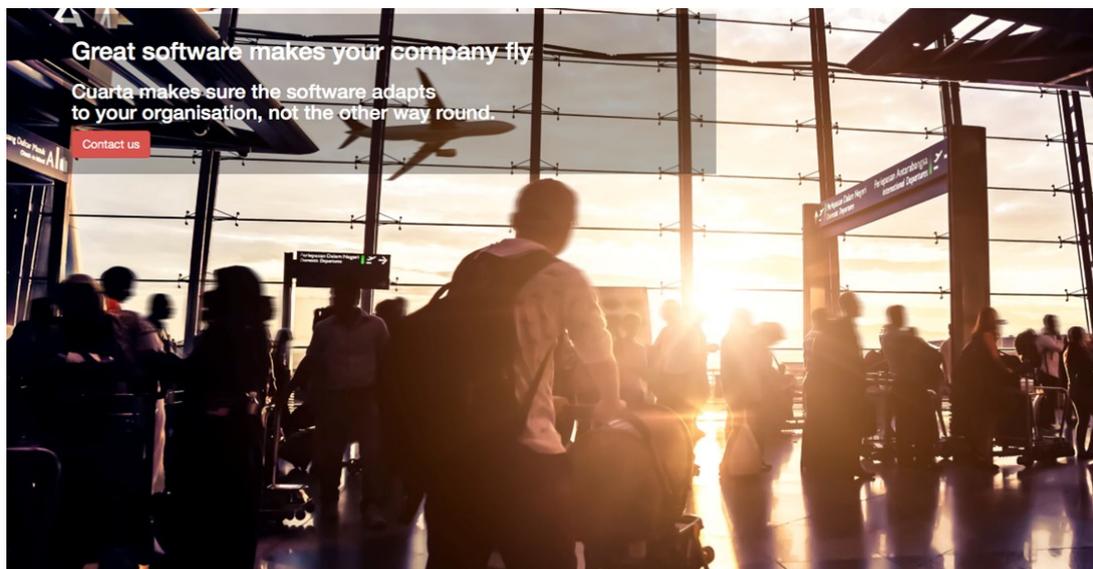
E2S ATO tool supports trade off of thousands of design variants

At the end of the second year of the project, we refined our ATO product from a UML modelling tool to a tool supporting rework, redesign and handling of variants. Another important feature is the fully customisable UML safety profile that can be edited using the ATO profile editor and that can cope with many specifics of safety development in a given context.

These were important steps but the support was still rather manual and not really scalable to a large amount of variants. So the true objective of the MERgE project was only met in small and isolated cases.

In the final and third year, we added an import facility so that designs from other tools can be imported. The ATO profile now also supports fully customisable checking and metrics facilities and the ability to run them in an automated way. This supports the trade off activity, analysing large sets of design variants. The end result is that ATO can now be used in the Merge tool chain on an industrial scale.

E2S also acquired another company mid 2015 so that E2S is now part of the Cuarta group. ATO fully supports one of the Cuarta missions to make sure that software engineering can be tuned to the business needs.



MERgE consortium

Follow
@MERgE_Project

Subscribe
<http://www.merge-project.eu/mailling-list>

Contact sanja.aaramaa@oulu.fi for more information about the articles above or potential joint dissemination activities.

Contact charles.robinson@thalesgroup.com for other MERgE matters.



Within the "Engineering support" theme of ITEA2 roadmap, the purpose of this project is to develop innovative concepts and design tools for multi-concern engineering when designing complex systems. The applicability and benefits of these innovations will be demonstrated in particular with "safety" and "security". Other concerns such as performance, reliability and traceability will also be considered. Four concrete use cases from different domains are provided as suitable test environments: radio communication, automotive, aerospace and industrial control.